

Comments to the Draft Reserve Bank of India (Know Your Customer) Amendment Directions, 2026

On 11 September 2026, the Reserve Bank of India (RBI) released the “**Draft Reserve Bank of India (Know Your Customer) Amendment Directions, 2026**” (hereafter “**Draft Directions**”).

The Draft Directions propose an SoP to guide the actions of REs when responding to suspected mule activity. They actively discourage REs from arbitrarily freezing accounts and call for restraint and proportionate interventions in response to warnings of suspicious activity.

In this response we present our comments to the Draft Directions, through 3 recommendations:

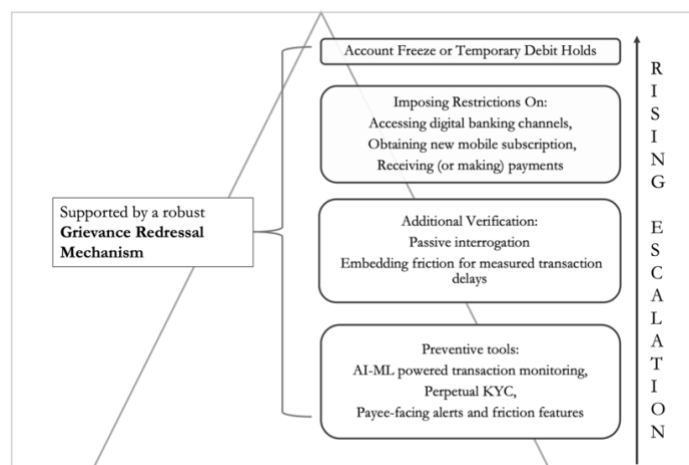
1. Definition of mule activity should be independent of static rules such as (fixed) transaction size (₹1,000).

The Draft Directions exclude activities below ₹1,000 from the definition of mule activity. We interpret this threshold of ₹1,000 as an exclusion criterion. While this may be justified where monitoring costs outweigh the disputed amounts, it also creates an incentive for fraudsters to keep transactions below the threshold. Such a rule risks overlooking suspicious activity that becomes apparent only when transactions are assessed together. For instance, repeated credits of ₹800 from unrelated accounts, followed by rapid outward transfers, may indicate mule activity despite each transaction falling below the threshold. Monitoring may therefore benefit from tracking account-level patterns like transaction frequency, velocity and deviations from routine customer behaviour. Drawing on multiple indicators in real time enables regulated entities and law enforcement agencies to recognise suspicious patterns as fraudsters adapt their strategies to evade static rules. We submit that the definition of suspected mule activity should be independent of transaction size and monitoring of transactions be guided by overall transaction patterns.

2. Regulated entities may consider a progressive-escalation matrix to guide their actions in responding to suspicious transactions.

We welcome the Draft Directions’ emphasis on REs’ discernment when imposing temporary debit holds or account freezes. To balance the need for swift interventions against the need to protect customers from arbitrary restrictions, we recommend REs embed a graduated approach in their internal policies, ensuring that account freezes are justified by evidence and adhere to due process. To this effect, we propose a progressive-escalation matrix that ranks tools available to REs from least to most restrictive.

The matrix envisages four levels of RE-interventions: (i) preventive action, (ii) additional verification, (iii) further restrictions, (iv) temporary holds and account freezes. The intensity of intervention should be proportionate to the strength of evidence, potential customer harm and risks to the financial system. The figure below depicts the progressive-escalation matrix.



Clear communication, prompt reversal of wrongful or excessive restrictions, and clarity on avenues of appeal, including the RBI Ombudsman, are essential complements to the effective execution of the progressive-escalation matrix.

3. The SoP may consider instituting a customer compensation framework.

Several Indian Courts have recognised customers' right to relief where banks freeze accounts arbitrarily or violate due process. We recommend that the Draft Directions contemplate a compensation framework that requires banks to compensate customers for breaches of the prescribed SoP or internal policies, or for disproportionate restrictions. Such a framework may be embedded in the SoP or could be incorporated into RE's internal policies. Drawing on the UK's approach, compensation decisions may account for the quality and strength of evidence of fraud, proportionality of measures undertaken by the RE, communication provided to the customer and customers' responses to it. Compensation relief could cover financial losses, distress and consequential harm, including damage to credit ratings. Further, designating the RBI Ombudsman as an appellate authority with redressal powers would strengthen customer protection and incentivise proportionate enforcement practices.

Discussion of Recommendations

1. Recommendation#1: Definition of mule activity should be independent of static rules such as transaction size (₹1,000).

The Draft Directions define suspected money mule transactions as "transactions which are ₹1,000 and above, flagged by the RE's transaction-monitoring systems (including AI / ML-based tools), as suspected to be proceeds of money mule activity." We interpret the ₹1,000 threshold to operate as an *exclusion criterion*. This may be justified on several grounds including public economics, when monitoring costs may outweigh the disputed amount, thus amounting to "throwing good money at bad money".

However, a rule-based exclusion criterion can create further perverse incentives in the system. It incentivises mule activity to cluster below the ₹1,000 limit, to evade monitoring. It is now widely accepted that static, rule-based triggers "overfit" historical patterns of fraud. They also do not have built-in flexibility or intuition for them, to adapt to changing fraud patterns.¹ This is in stark contrast with modus operandi of fraudsters, who continually improvise their strategies in response to static rules, such as by distributing abuse across accounts so each single event looks ordinary.² Rule-based exclusion criterion may create blind spots for REs and LEAs. These blind spots may especially occur where suspicious activity is manifested through multiple lower-value transactions.³ For instance, an account may receive multiple credits of ₹800, each from unrelated accounts within a short period, followed by similar low-level rapid transfers of funds to another account. In this case, although each individual transaction falls below the ₹1,000 threshold, the frequency, velocity or pattern of the transactions may collectively indicate potential money-mule activity. A transaction-level threshold, if applied in isolation, may fail to capture suspicious patterns that become apparent at account level assessment.

Exclusion criterion or triggers should therefore supplement transaction ticket-size with other account-level patterns, such as transaction velocity, frequency and deviations from customer's routine behaviour. For example, the Singapore Shared Responsibility Framework, flags transactions when a transaction, together with withdrawals made in the preceding 24 hours, exceeds 50% of the account balance. This decision is made in conjunction with enhanced monitoring by the RE and LEA, where account-level factors are considered to identify suspicious transactions.⁴ Such triggers are sensitive to individual account activity and steer clear of universal rules that are blunt and vulnerable to being gamed.

We submit that transaction patterns, determined by a suite of real-time indicators may be a superior indicator of suspicious activity than the transaction size alone. Therefore, a framework in which the definition of mule activity is independent of transaction size (and other static rules) may be more effective in identifying suspicious activities and mitigating them.

2. Recommendation#2: Regulated entities may consider a progressive-escalation matrix to guide their actions in responding to suspicious transactions.

The Draft Directions encourage REs to exercise discernment when enforcing temporary debit holds or more enduring account freezes. We welcome this steer. Our research on effective enforcement mechanisms in other sectors suggests that RE's interventions can benefit from adopting the risk-responsive regulation paradigm. To this end, we propose a progressive-escalation matrix that arranges the tools available to REs from least to most restrictive.

¹ <https://www.thehindubusinessline.com/opinion/remedies-for-digital-payment-frauds/article70948012.ece>

² <https://nhimg.org/faq/what-happens-when-fraud-detection-relies-on-static-rules-instead-of-adaptive-sig/>

³ <https://euro.econ.cm.u.edu/resources/elibrary/epay/s10618-008-0116-z.pdf>

⁴ https://abs.org.sg/docs/library/banks-to-launch-enhanced-safeguards-from-15-oct-2025-to-better-protect-accounts_.pdf

A temporary debit hold is certainly preferred to the complete freezing of bank accounts⁵. However, even temporary holds affect customer rights. Therefore, a progressive-escalation mechanism as espoused in the risk-responsive regulation paradigm⁹ may strike a balance between the need for swift interventions and the restraint that is warranted to ensure innocent customers' accounts are not suspended arbitrarily.

When guided by a progressive-escalation matrix, the RE's the choice of intervention would be proportionate to the likelihood of the transaction being suspicious, the risk posed to the systems and customers, the interconnectedness of the transaction, the certainty of the recipient being a criminal etc. The greater the probability of a transaction being suspicious, the more prohibitive and expensive the sanctions on the transaction beneficiary. A complete suspension of account activities, in this case would be justified by a very high probability of the payment activity being fraudulent.¹³ Such a graduated response is common among financial systems, in India and globally.¹⁴ Further, progressive escalation can be used to design preventive measures also.

Such progressive escalation allows us to: (i) establish a continuum of interventions before resorting to account-level freezing; and (ii) calibrate the nature of RE's interventions to the strength of available evidence, the potential risk to the customer, and the financial system.

Implementing the progressive-escalation matrix:

The matrix envisages four levels of RE-interventions: (A) preventive action, (B) additional verification, (C) further restrictions, (D) temporary holds and account freezes.

A. Preventive Action: Ex-ante measures are integral to the progressive-escalation matrix. Preventing suspicious activities helps REs avoid expensive sanctions later and win over customers' trust.^{6,7} Preventive action comprises real-time transaction and KYC monitoring and alerting payees. We discuss these next.

- **Monitoring systems:** Dynamic indicators like changes in transaction velocity, behavioural or biometric patterns, geographical locations and devices used, and other contextual information, when considered together are effective indicators of suspicious activity.⁸ Several systems already own and deploy such capabilities. The NPCI, reportedly uses AI-powered tools to test the veracity of each transaction.⁹ Similarly, RBI-H's MuleHunter¹⁰ uses similar patterns to detect mule activity. Further, REs also contribute to and harvest system-level intelligence through platforms like I4C's CFCFRMS, RBI's DAKSH and DPIP.

Robust KYC process is also an important preventive action tool. Currently, KYC is a static profiling tool, updated periodically, in consonance with customers' risk profile.¹¹ Notably, Jan Dhan accounts, which require KYC updates only once every ten years, are emerging as a fertile catchment for mule activity.¹² This trend supports the arguments made in #1, that static rules create perverse incentives and encourage fraudsters to leverage any forbearance afforded by the rules. Revamping KYC, and orienting towards Perpetual KYC¹³ could help address these concerns. Globally, policies such as the UK's policy

⁵ <https://www.livelaw.in/high-court/calcutta-high-court/rbi-guidelines-do-not-specifically-authorise-banks-to-freeze-accounts-on-mere-suspicion-of-money-mule-activity-calcutta-high-court-549563>

⁶ <https://www.credit-connect.co.uk/news/consumer-lending/financial-services/consumers-prioritising-fraud-protection-when-selecting-financial-services/>

⁷ <https://www.alloy.com/blog/protection-as-a-product-fraud-prevention-trust-banking>

⁸ <https://dvararesearch.com/wp-content/uploads/2026/05/Comments-to-the-Discussion-Paper-Exploring-safeguards-in-digital-payments-to-curb-frauds.pdf>

⁹ <https://www.billcut.com/blogs/new-npci-alerts-fewer-upi-payment-scams/>

¹⁰ <https://rbihub.in/projects/mulehunter>

¹¹ <https://www.rbi.org.in/commonman/english/scripts/notification.aspx?id=2607#9>

¹² <https://the420.in/jan-dhan-accounts-cyber-fraud-mule-network-22-crore-pune-scam/>

¹³ <https://dvararesearch.com/from-periodic-to-perpetual-rethinking-the-process-of-kyc/>

on fraud prevention¹⁴ advocates for REs to move away from a static approach for KYC (as seen in the risk categorizations of customers). A Perpetual KYC system would include an almost continuous, near real-time scrutiny of customers' risk profile.¹⁵ This would update customers' risk profile frequently and automatically graduate riskier customers to greater scrutiny, regardless of static indicators such as income levels or the types of account.

- **Alerting prospective victims:** Payee-facing interventions such as alerts, warnings or mandatory lags in payment authorisations prevent fraudulent transactions by counteracting impulsive transfers by payees.

B. Graduated response to potentially suspicious transactions: This is the second level of escalation. Here, REs calibrate their response to fraud alerts (generated internally or externally) basis the quality of the evidence.

- **Additional verification:** As a first response to a potential suspicious activity, REs may undertake passive, non-interrogative intelligence-gathering. This could include examining the source and purpose of the transaction, the nature of the relationship between the parties, shared account details and whether the recipient is a known or reported fraud victim.¹⁶ Such additional verification is already contemplated within the RBI's risk-management and transaction-monitoring framework, which requires banks to undertake appropriate customer contact and verification measures where necessary. This may also be complemented by proportionate friction, such as a cooling-off period or time lag, enabling REs to undertake further due diligence.^{17,18} While these friction measures resemble the ex-ante features, it is worth noting that at this stage, these measures are implemented on a case-by-case basis and in response to specific suspicious-transaction warnings.
- **Imposing further restrictions:** As the evidence of the activity being fraudulent grows stronger, REs may resort to more expensive, inhibitory interventions to delay or temporarily suspend specific transactions. Singapore's Protection of Scams Act (Scams Act), 2025 enables risk-calibrated restrictions on mules' access to (i) digital banking, card/ATM transactions; (ii) new mobile lines; and (iii) registering for higher-risk services that could be exploited for scams. The restrictions aim to limit, in a risk-proportionate manner, the access to channels through which scam proceeds may be transferred.¹⁹

C. Holds and Freezes: RE's can resort to temporary holds and account freezes when there is high-quality evidence indicating a strong likelihood of the account or activity being fraudulent. While the Draft Directions already lay out conditions for holds and freezes, REs' internal policies should also account for emerging jurisprudence on determining the need for account freezing. The Rajasthan High Court in *Shree Balaji Enterprises v. RBI* (2026) lays out four preconditions for freezing bank accounts in this context:

- there must be lawful authority for the restraint;
- there must be tangible material disclosing a prima facie nexus between the account or transaction and the offence under investigation;
- the investigating officer must identify, as far as reasonably practicable, the transaction and amount requiring protection; and
- the restraint must be proportionate to the investigative necessity and cannot continue mechanically after the necessity ceases to exist.

¹⁴ <https://www.gov.uk/government/news/new-measures-to-tackle-fraud-come-into-effect>

¹⁵ (i) <https://dvararesearch.com/from-periodic-to-perpetual-rethinking-the-process-of-kyc/>

¹⁶ <https://cdnbbsr.s3waas.gov.in/s3ec03936824c0191953647ec609b4f49b/uploads/2026/06/2026061955.pdf>

¹⁷ <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12770&Mode=0>

¹⁸ (i) <https://fintech.global/2024/10/07/uk-banks-to-hold-suspicious-payments-for-72-hours-to-combat-fraud/> (ii)

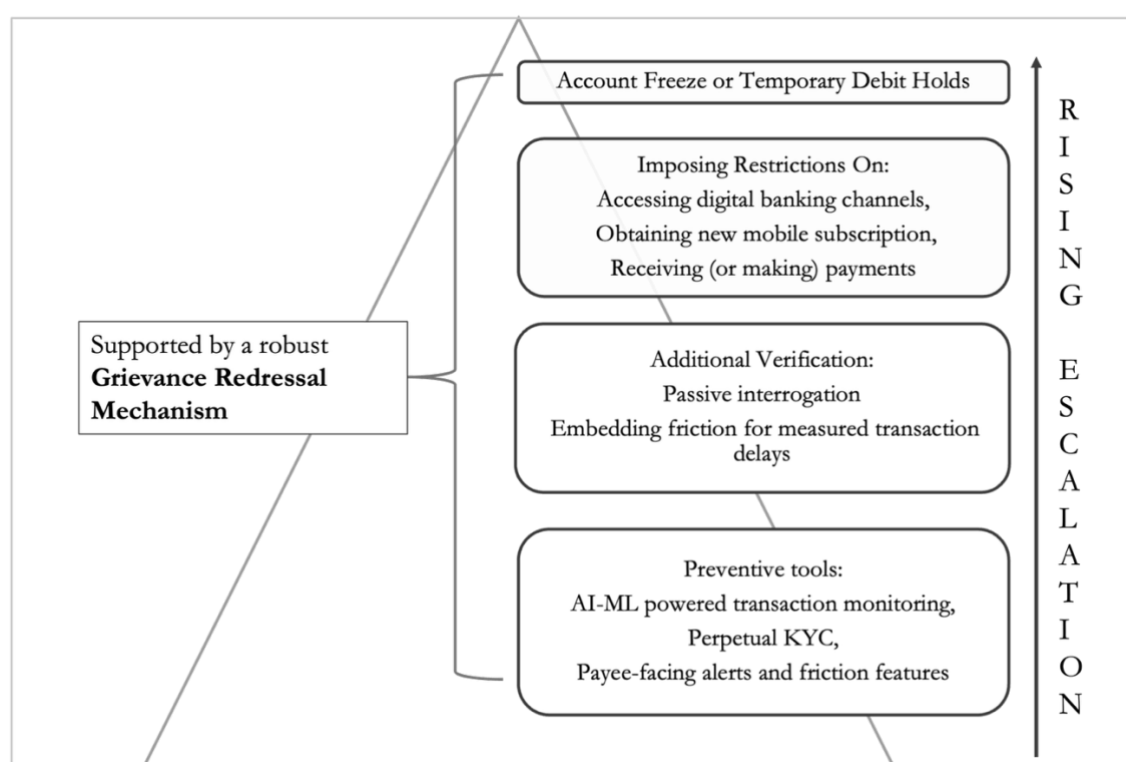
<https://www.dbs.com.sg/personal/support/general-digibank-security-cooling-period.html>

¹⁹ <https://www.mas.gov.sg/news/media-releases/2025/joint-press-release-by-spf-mas-imda-and-govtech-on-restricting-access-to-facilities-for-scam-mules>

From the above, it is imperative that freezes and hold-ups be reversed swiftly where warranted. The Draft Directions already emphasise the need for a grievance redress mechanism and lay out a timeline for customer communication and the reversal of hold-ups and freezes.

We submit that REs could benefit from contemplating, a progressive-escalation matrix that comprises a wide range of risk-proportionate interventions. This would equip REs to calibrate their response to the strength of the evidence of suspicious activity. Attention must also be paid to the design of the grievance redressal mechanism. An accessible, proactive and prompt grievance redress is a necessary pre-requisite for implementing these sanctions. Also, clarifying existence of the appellate authority, the RBI Ombudsman, in this regard would further secure the rights of customers. Figure 1 depicts the progressive-escalation matrix of interventions that REs may consider embedding in their internal policies.

Figure 1: A progressive-escalation matrix of a suite of interventions that can guide REs in responding to suspicious transactions and mule activity.



3. Recommendation#3: The SoP may consider instituting a customer compensation framework.

Recently, several High Courts have instructed banks to compensate customers where customer accounts were frozen unnecessarily or without regard to the due process of the law.^{20,21} In other instances, the Courts have also recognised that unilateral account freezing by banks could amount to *deficiency in service*, under the Consumer Protection Act, 2019.²² These instances already indicate that the Courts recognise customers' rights to relief when banks violate due process during account freezing.

²⁰ <https://www.lexology.com/library/detail.aspx?g=6cc6038a-0d36-4c21-b4a0-53fd3174868d>

²¹ <https://www.legal500.com/intelligence/india/finance-and-banking/banks-as-custodians-not-arbiters-karnataka-high-court-reaffirms-proportionality-in-account-freezing-orders>

²² <https://www.mirzaandassociates.com/bank-account-freezes-in-cyber-fraud-complaints-navigating-judicial-safeguards-and-remedies-for-businesses/>

We submit that Draft Directions may contemplate a customer compensation framework that grants relief to customers when banks violate the SoP or internal policies or when the banks' actions are disproportionate and cause unreasonable losses or inconveniences to customers.

The UK's Financial Conduct Authority (FCA), for instance, determines the disproportionality of banks' decision to suspend/block/freeze transactions through a wide range of factors: strength of the evidence, likelihood and severity of harm to customer and the system, quality of communication to the customer and the consideration given to the customers' response, etc.²³ Where banks are found responsible, the Financial Ombudsman reserves the rights to offer awards to customers.²⁴ Awards may include:²⁵ (i) covering any or all costs that the customer may have incurred such as late payment fee or interest; (ii) monetary awards for any harassment or embarrassment, (iii) directions including correcting credit ratings that were affected because of customers' inability to pay due to account suspension.

We recommend including a compensation framework in the SoP or encouraging REs to incorporate one in their internal policies. Further, reiterating the role of the Integrated Ombudsman as the appellate authority with redressal powers would safeguard customers' rights and create incentives for adherence of the SoP.

About Dvara Research

Dvara Research is an independent, non-partisan, not-for-profit policy research institution based in India. Its mission is to ensure that every low-income household and every small enterprise has complete access to suitable financial services and social security through a range of channels that enable them to use these services securely and confidently.

Since 2008, Dvara Research has deeply analysed, and carefully written about, financial inclusion and social protection in India from policy, regulatory, and practitioner perspectives that are anchored to its mission. Its work has gained the admiration and respect of policymakers and regulators, and since its inception, Dvara Research has been a research-partner of choice for such key policy-making bodies as the Reserve Bank of India, Securities and Exchange Board of India, Pension Fund Regulatory and Development Authority etc.

Website: <https://dvararesearch.com>

²³ <https://www.fca.org.uk/freedom-information/information-freezing-orders-under-poca-july-2022>

²⁴ <https://www.financial-ombudsman.org.uk/businesses/resolving-complaint/understanding-compensation>

²⁵ *supra*